

الذكاء الاصطناعي والأمن السيبراني:
دراسة فيما يخبئه المستقبل

ألبانا إيسيني

ترجمة وتحرير مركز البيان للدراسات والتخطيط

عن المركز

مركزُ البيان للدراسات والتخطيط مركز مستقلٌّ، غيرُ ربحيّ، مقرّه الرئيس في بغداد، مهمته الرئيسة -فضلاً عن قضايا أخرى- تقديم وجهة نظر ذات مصداقية حول قضايا السياسات العامة والخارجية التي تخصّ العراق بنحو خاصٍ ومنطقة الشرق الأوسط بنحو عام. ويسعى المركز إلى إجراء تحليل مستقلّ، وإيجاد حلول عمليّة جليّة لقضايا معقدة تهمّ الحقليْن السياسي والأكاديمي.

ملاحظة:

الآراء الواردة في المقال لا تعبر بالضرورة عن اتجاهات يتبناها المركز، وانما تعبر عن رأي كتابُها.

ترجمة: د. باسم علي خريسان

www.bayancenter.org
info@bayancenter.org

Since 2014

الذكاء الاصطناعي والأمن السيبراني:
دراسة فيما يخبئه المستقبل

ألبانا إيسيني *

يجب أن يكون تكامل البرمجيات والحلول التقنية واستخدامهما مصحوباً بإجراءات أمنية ذات صلة، فالأمن السيبراني صناعة متنامية باستمرار، تتطوَّر لحماية الأفراد والمؤسسات من الهجمات السيبرانية. أصبح الذكاء الاصطناعي (AI) ببطئ جزءاً لا يتجزأ من الأمن السيبراني، ممَّا يساعد المؤسسات ذات الأحجام والصناعات المختلفة على زيادة كفاءة الأمن السيبراني.

تكنولوجيا المعلومات والاتصالات هي الصناعة الأسرع والأكثر تقدماً في عملية تبنِّي الذكاء الاصطناعي، وتُستخدم خوارزميات الذكاء الاصطناعي، والتعلُّم الآلي اليوم لأتمتة المهام، ومعالجة البيانات، وتحسين الأمن السيبراني، واتخاذ القرارات بسرعة مستحيلة بشرياً.

واستناداً للإحصائيات عبر الإنترنت، من المتوقَّع أن ينمو السوق العالمي للذكاء الاصطناعي في مجال الأمن السيبراني بمعدَّل CAGR (معدل النمو السنوي المركب)[1] (23.6٪) إبَّان 2020 إلى 2027، ليصل إلى (46.3) مليار دولار، وَفْقاً لمؤسسة البيانات الدولية (IDC)[2]، سيصل الإنفاق العالمي على الأمن السيبراني إلى (174.7) مليار دولار في عام 2024، مع عدِ

1 – معدل النمو السنوي المركب (CAGR): هو متوسط معدل نمو استثمار ما خلال فترة زمنية محددة تفترض «مضاعفة» (إعادة استثمار الأرباح في كل فترة زمنية خلال تلك الفترة الزمنية) التي تسهل كيف ينظر نمو الشركة إلى رقم واحد كما لو كان النمو قد حدث بصورة مطردة كل عام خلال تلك الفترة الزمنية، يستخدم معدل النمو السنوي المركب (CAGR) عادةً بوصفه أداة لتقييم أداء الأسهم أو الاستثمار خلال فترة زمنية محددة في الماضي، إنَّها إحدى الطرائق التي يمكنك عن طريقها حساب معدَّل نمو الأسهم أو يمكن لصاحب رأس المال الاستثماري تقييم أداء شركة ناشئة أنَّه متوسط مقدار مكاسب الاستثمار أو خسارته على أساس سنوي (أو مستوى اعتيادي آخر). https://www.almrsal.com/post/1096089

2 – شركة البيانات الدولية (IDC): هي المزود العالمي الأول لمعلومات السوق والخدمات الاستشارية والأحداث الخاصة بتكنولوجيا المعلومات والاتصالات وأسواق تكنولوجيا المستهلك، مع أكثر من (1200) محلل في جميع أنحاء العالم، تقدِّم IDC خبرات عالمية وإقليمية ومحلية في التكنولوجيا والفرص الصناعية والاتجاهات في أكثر من (110) دولة، يساعد تحليل IDC ورؤيته المتخصصين في مجال تكنولوجيا المعلومات والمديرين التنفيذيين ومجتمع الاستثمار على اتخاذ قرارات تقنية قائمة على الحقائق وتحقيق أهداف أعمالهم الرئيسة، أُسِّست IDC في عام 1964، وهي شركة فرعية مملوكة بالكامل لمجموعة International Data Group (IDG، Inc)، الشركة الرائدة عالمياً في مجال الإعلام التكنولوجي وخدمات البيانات والتسويق: https://www.idc.com/about

* مدير أول لتسويق المنتجات في RSI في BCEP. وهي مسؤولة عن إجراء أبحاث السوق أثناء تطوير المعلومات المتعلقة بمعايير OSI وتقديمها.

خدمات الأمن القطاع الأكبر والأسرع نمواً.

سيؤدِّي هذا النمو إلى زيادة أهمية الذكاء الاصطناعي في الأمن السيبراني ومكافحة التهديدات الأمنية الكبرى التي يجب البحث عنها في عام 2022، ومع ذلك، فإنَّ الاعتماد على هياكل ومنصات الذكاء الاصطناعي لا يخلو من التحديات، إذ إنَّ (60٪) من المنظمات التي أدرجت الذكاء الاصطناعي في الأمن السيبراني اعترفت بمخاطره بوصفه الأكثر انتشاراً.

تكامل الذكاء الاصطناعي في الأمن السيبراني

يُعدُّ الذكاء الاصطناعي أحد الأصول الحاسمة للمنظمات التي تستخدم الأتمتة من أجل زيادة إنتاجية عملياتها وفعَّاليتها، وَوَفْقاً لشركة IBM، فإنَّ أحد التطبيقات المهمة التي تستفيد من الذكاء الاصطناعي أكثر من أي تطبيق آخر اليوم هو أمن البيانات أو الأمن السيبراني، مع زيادة التحوُّل الرقمي بسرعة، يزداد عدد خروقات البيانات وتطورها. يمكن أن يكون الذكاء الاصطناعي أداةً قويةً في الحماية من الهجمات السيبرانية.

الوظائف الرئيسة للذكاء الاصطناعي في الأمن السيبراني

1–الكشف: تستخدم المنظمات الذكاء الاصطناعي بصورة أساسية؛ للكشف عن التهديدات السيبرانية، وَوَفْقاً لبحث أجرته [3] (Capgemini، فإنَّ أكثر من (50٪) من المؤسَّسات التي طبقت حلولاً للأمن السيبراني قائمة على الذكاء الاصطناعي، تستخدمها لأغراض الكشف عن التهديدات، ويرجع ذلك إلى القدرات الفريدة للذكاء الاصطناعي لتحديد حركة المرور غير المنتظمة عن طريق التعلُّم الآلي أو التعلُّم العميق.

2–التنبُّؤ: يستخدم عدد كبير من المنظمات الذكاء الاصطناعي للتنبؤ بالتهديدات السيبرانية، يكون ذلك عن طريق مسح البيانات وإجراء تنبؤات بناءً على تدريب النظام، يمكن للمنظمات التي تتبنَّى الذكاء الاصطناعي لأغراض التنبؤ –أيضاً– أن تستخدم التكنولوجيا؛ لتحديد نقط الضعف

3 – Capgemini: هي شركة عالمية رائدة في الشراكة مع الشركات لتحويل وإدارة أعمالها عن طريق تسخير قوة التكنولوجيا. تسترشد المجموعة كل يوم بهدفها المتمثل في إطلاق العنان للطاقة البشرية عن طريق التكنولوجيا من أجل مستقبل شامل ومستدام. إنَّها منظمة مسؤولة ومتنوعة تضم (300000) عضو في الفريق فيما يقرب من 50 دولة. بفضل تراثها القوي لـ 50 عاماً وخبرتها العميقة في الصناعة، تحظى Capgemini)) بالثقة من قبل عملائها لتلبية النطاق الكامل لاحتياجات أعمالهم، من الإستراتيجية والتصميم إلى العمليات، مدعوماً بالعالم سريع التطور والمبتكر للسحابة والبيانات والذكاء الاصطناعي والاتصال والبرمجيات والهندسة الرقمية والمنصات. أعلنت المجموعة في عام 2020 عن عائدات عالمية بقيمة 16 مليار يورو:
https://ae.linkedin.com/company/capgemini

الحرجة، وتحديد أصول وطوبولوجيا[4] الشبكة تلقائياً، وتحسين دفاعات شبكاتها باستمرار ضد أي هجمات سيبرانية محتملة.

3–الاستجابة: تتطور أنماط الذكاء الاصطناعي للاستجابة للتهديدات السيبرانية باستمرار، يمكن للمؤسسات الآن استخدام الذكاء الاصطناعي؛ لاكتشاف الهجمات وإيقافها في الوقت نفسه، ويمكنهم أتمتة إنشاء رقعة افتراضية للتهديد المكتشف أو تطوير آليات حماية جديدة في الوقت الفعلي، يساعد الذكاء الاصطناعي المنظمات على خفض التكاليف وتحسين وقت الاستجابة للتهديدات والاستجابة للانتهاكات، بغض النظر عن الأنماط أو الأساليب أو الخصائص المحدَّدة التي تُستخدم فيها.

تحديات الذكاء الاصطناعي في الأمن السيبراني

يأتي تكامل الذكاء الاصطناعي في أنظمة الأمن السيبراني مع بعض العوائق والقيود، وأكثرها شيوعاً استخدام مجرمي الإنترنت للذكاء الاصطناعي وحواجز التبني.

يجعل استخدام الذكاء الاصطناعي من قبل مجرمي الإنترنت الذكاءَ الاصطناعي سلاحاً ذو حدين، يمكن استخدامه بوصفه أداةً وقائية قوية، فضلاً عن آلية هجوم قوية، على الجانب الهجومي، يمكن للمهاجمين استخدام الذكاء الاصطناعي لزيادة دقَّة هجماتهم وفاعليتها، تلتزم المنظمات التي تتبنى الذكاء الاصطناعي في أنظمة الأمن السيبراني الخاصة بها بلوائح محددة، والتي غالباً ما تحد من نطاق استخدامها.

في المقابل، يتمتع مجرمو الإنترنت بمساحة لعب غير محدودة، ممَّا يسهِّل عليهم الاستفادة من التكنولوجيا لأغراض ضارة، أحد أشهر تقنيات تحليل البرامج التي يستخدمها المتسلِّلون هو «التشويش»، يُستخدمُ هذا في الغالب للعثور على الثغرات الأمنية في البرامج المعقدة، الهدف الرئيس من هذه التقنية هو التسبُّب بحدوث تجاوزات في المخزن المؤقت، وأعطال، وأخطاء في الذاكرة، واستثناءات وكشف نقط ضعف النظام.

4 – «هو أحد فروع علم الرياضيات والذي يهتم بدراسة تراكيب و مكونات و خصائص جميع الفضاءات المختلفة، إذ تبقى هذه الخصائص متشابهة تحت عمليات التشكيل المتصلة (Smooth Deformations) من دون أن يقوم بعملية تمزيق أو يترك فتحات في الانتقال من أحدهما إلى الآخر و بالعكس أيضاً».
https://www.salmimath.com/2017/12/Topology.html

يزيد استخدام الذكاء الاصطناعي بهذه التقنية من دقة الهجوم وكفاءته، ومن ثَمَّ خلق تهديد مدمِّر، يمكن أيضاً استخدام الذكاء الاصطناعي في هجمات التصيد الاحتيالي، ويتميَّز التصيُّد الاحتيالي المدعوم بالذكاء الاصطناعي بزيادة سرعة التنقُّل في البيانات الحسَّاسة وتقليل حركة المرور، يساعد هذا مجرمي الإنترنت في استخراج المعلومات الضرورية فقط، ويجعل اكتشاف البرامج الضارة أصعب.

حواجز التبني

مع الأخذ بنظر الاعتبار، يمثِّل الذكاء الاصطناعي صناعة جديدة، تحتاج المؤسسات إلى استثمار قدر كبير من المال والوقت في قوة الحوسبة والذاكرة ومراكز البيانات؛ لتكون قادرة على بناء أنظمة الذكاء الاصطناعي وصيانتها، مع ذلك؛ ومع تقدِّم التكنولوجيا، تنخفض التكاليف، ممَّا يجعل الخوادم عالية الجودة سهلة التناول.

لقد أصبح دمج الذكاء الاصطناعي في الأمن السيبراني أمراً لا غنى عنه للمنظمات، ومع ذلك فإنَّ العوائق الرئيسة التي تبطِّئ من اعتماده ونشره هي الحاجة لاكتساب المواهب، وتعقيد البيانات وتوظيف أدوات الذكاء الاصطناعي المناسبة، وفقاً لشركة IBM، فإنَّ أحد أهم عوائق نشر الذكاء الاصطناعي هو نقص المواهب، إذ أكَّدت حوالي (37٪) من المنظمات صعوبة العثور على أشخاص يتمتعون بالمستوى المناسب من الخبرة والمعرفة في مجال الذكاء الاصطناعي، وهذا مهم للغاية للمنظمات التي بالكاد بدأت في تبني الذكاء الاصطناعي، وبما يخص المؤسسات التي هي في مراحل متقدمة من نشر الذكاء الاصطناعي، فإنَّ تعقيد البيانات وامتلاك مجموعة الأدوات المناسبة هي العقبات الرئيسة.

مستقبل الأمن السيبراني: فجوة متزايدة في المهارات

تحتاج المنظمة التي تنفِّذ دفاعات قوية ضد الهجمات السيبرانية إلى قوى عاملة ماهرة وذات خبرة في مجال الأمن السيبراني، وهو أمر ليس من السهل العثور عليه؛ نظراً للطلب الكبير على الأشخاص الماهرين في هذا المجال.

ويتزايد عدد الأفراد المهتمين بأخذ دورات في الأمن السيبراني، ومن المتوقَّع أن ينمو هذا الاتجاه أكثر في المستقبل، إذ إنَّ الطلب أعلى بكثير من العرض، ولا بدَّ من التأكيد على أنَّ

الهجمات السبرانية سوف تزداد باستمرار إذا تركت من دون رقابة، وستصبح أخطر، ويمكن منع ذلك عن طريق الاستثمار الكبير المستمر في الأشخاص المتخصصين بصد هذه الهجمات، الأمر الذي يمكن أن يكون عن طريق تعيين خبراء الأمن السيبراني أو عن طريق تدريب الموظفين على دمج الذكاء الاصطناعي في أنظمة الأمن السيبراني[5].

رابط الدراسة:

https://pecb.com/article/artificial-intelligence-and-cybersecurity-what-the-future-holds



5- https://pecb.com/article/artificial-intelligence-and-cybersecurity-what-the-future-holds.